



第六十五届会议

暂定项目表\* 项目 94

从国际安全的角度来看信息  
和电信领域的发展

从国际安全的角度来看信息和电信领域的发展

秘书长的报告

目录

	页次
一. 导言 .....	2
二. 从各国政府收到的答复 .....	2
古巴 .....	2
希腊 .....	5
墨西哥 .....	6
巴拿马 .....	8
卡塔尔 .....	8
乌克兰 .....	10
大不列颠及北爱尔兰联合王国 .....	13

\* A/65/150。



## 一. 引言

1. 大会在第 64/25 号决议第 3 段，邀请所有会员国继续向秘书长通报其对下列问题的看法和评估意见：

- (a) 对信息安全的一般看法；
- (b) 国家一级为加强信息安全和促进这一领域的国际合作所作的努力；
- (c) 该决议第 2 段所述概念的内容；
- (d) 国际社会为加强全球一级信息安全可能采取的措施。

2. 按照这项要求，2009 年 2 月 27 日向各会员国寄发了一份普通照会，请它们就这一主题提供资料。所收到的答复载于下文第二节。以后再收到的其他答复将作为本报告增编印发。

## 二. 从各国政府收到的答复

### 古巴

[原件：西班牙文]  
[2010 年 5 月 27 日]

1. 古巴完全赞同大会第 64/125 号决议中所表达的关于以下方面的关切：信息技术和媒体可能会被用于不符合维护国际稳定与安全宗旨的目的，可能对别国基础设施的完整性产生不利影响，损害其民用和军事领域的安全。该决议还适当地强调了有必要防止为犯罪或恐怖主义目的利用信息资源或技术。
2. 古巴重申，充满敌意地使用电信并公开或隐蔽地意图破坏别国的法律和政治秩序的做法，违反了有关此问题的国际公认准则，也是负面和不负责任的，可能会引起紧张局势和不利于国际和平与安全的情况，从而破坏《联合国宪章》所体现的原则和宗旨。
3. 古巴关切地提请关注下列事实，即当信息和电信系统被设计和/或被用于破坏别国基础设施时，这些系统就可能变成武器，从而危及国际安全与和平。
4. 在这方面，古巴重申其在不同国际论坛上表达过的谴责，即谴责历届美国政府通过对古巴开展广播和电视战，使这一侵略不断升级。这明显违反现行的管理无线电频谱的国际规则。
5. 美国政府毫不顾忌其可能对国际和平与安全造成危害，比如通过制造危险状况如未经协议而使用军用飞机向古巴传送电视信号。

6. 从美国领土对古巴发动广播-电子侵略违反了规范国家间关系的国际法以及国际电信联盟(国际电联)的准则和规章,这些法律法规规定了联合国系统这一专门机构的成员国应该采取的行动。

7. 每个星期,位于美国领土的广播电台在 34 个不同的中波、短波、调频和电视频率,传送上千小时的广播和电视节目。2010 年 3 月,每星期非法传送 2 156 小时的节目。其中一些广播公司属于与广为人知的恐怖分子有关联的组织或为其提供服务,这些恐怖分子住在美国领土并同美国当局达成全面协议,从事反对古巴的活动。

8. 针对古巴的非法广播和电视节目并不提供新闻;相反,是为了颠覆目的,而捏造和歪曲新闻。对于这种行为,美国国会每年从联邦资金中核准 3 000 万美元的预算。自两家广播公司开始活动以来,美国政府已为此目的花费 6 598 亿美元。

9. 对古巴的挑衅性广播违反了以下国际原则:

- 《国际电信联盟章程》序言部分的基本原则,即电信对于维护和平及所有国家的经济社会发展日益重要,通过有效的电信服务手段,实现促进各国人民间的和平关系与国际合作以及促进经济社会发展的目标。美利坚合众国政府对古巴播出的电视节目内容,具有颠覆性、破坏性和欺骗性,是与以上原则相抵触的。
- 《国际电信联盟章程》第 197 条和第 198 条规定,所有电视台都必须在不对其他成员国广播服务或通讯造成有害干扰的情况下,有效建立和运行。
- 2007 年 11 月举行的世界无线电通信大会第九届全会协议第 6.1 段(g)分段规定:“航空器运营的任何广播站,如系专门向该国政府领土播放而未经该国政府许可,则构成违反《无线电规章》”。
- 国际电信联盟《无线电规章》第 8 条第 8.3 款规定,其他国家政府在分配本国频率时,应考虑到已分配和登记并得到国际承认的频率,以避免有害干扰。
- 国际电信联盟《无线电规章》第 42.4 条,禁止在海面或其上空的航空器站进行任何无线电广播业务。
- 国际电信联盟无线电规章委员会在 2004 年 12 月第 35 次会议上提出的裁决指出,美国在 213 兆赫的广播对古巴节目服务造成有害干扰,并要求美国政府采取适当措施取消转播。自 2006 年 9 月以来,无线电规章委员会还一直要求美国政府采取有关措施,消除在 509 兆赫的干扰,但至今没有答复。2009 年 3 月 20 日,该委员会第 50 次会议及其决定概要(RRB09-1/5 号文件)再次重申,这些广播是非法的,并要求美国采取一

切必要措施，消除这两宗干扰古巴电视节目的情况。国际电信联盟无线电规章委员会在 2010 年 3 月 26 日第 53 次会议上，重申其结论，即从美国从事的广播对包括在国际频率登记册上的古巴广播电台造成有害干扰，并敦促美国当局消除该有害干扰，要求无线电通信局监测有关情况，并按《无线电规章》规定的程序采取行动。

- 国际电信联盟《无线电规章》第 23.3 条限制向国外播放电视节目。

10. 2009 年 1 月美利坚合众国政府问责局(美国官方机构)发表的报告承认，美国政府对古巴的广播和电视节目违反了国际法准则和国内立法。

- 该报告回顾，国际电信联盟在 2004 年和 2006 年认定，美国在 13 和 20 频道的播放对古巴电台造成了有害干扰，而美国国务院没有采取任何行动回应国际电联的裁决。报告还指出，2007 年 11 月举行的世界无线电通信大会认为，从航空器播放的做法不符合国际电联规章。
- 该报告指出，尽管美国法律禁止在国内传播这种类型的广播节目，但在美国领土内、主要在迈阿密均能接收到这类的广播和电视转播，一些合同广播电视台播送政治广告和提供性服务产业的广告。另外，报告还注意到，对古巴的广播没有遵守新闻的平衡和客观标准，使用了煽动性和攻击性的语言。

11. 古巴进一步回顾，2007 年 10 月 22 日至 11 月 16 日在瑞士日内瓦举行的世界无线电通信大会通过的结论文件认定，美国从航空器对古巴的无线电播放违反了《无线电规章》。全体会议通过的结论规定：“从航空器上运营的任何广播站，如系专门向他国政府领土播放而未经该国政府许可，则被认定不符合《无线电规章》”。

12. 这些结论是世界无线电通信大会全会通过的，对国际电信联盟的工作具有法律效力。因此，世界无线电通信大会通过了 1990 年由当时的国际频率登记委员会所做的声明，即对航空气球针对古巴领土播放电视节目构成违反《规章》的规定。

13. 美利坚合众国政府对古巴的敌对态度，在其近 50 年来的经济、商业和金融禁运中彰显无疑，这一禁运也影响到信息和电信领域：

- 古巴无法获得许多网站提供的服务；只要链接被看出来自古巴 .cu 域名的因特网地址(IP)，就会遭到拒绝。
- 在没有事先通知的情况下，外国资产管制处(外资管制处)禁运了与古巴有联系的 .com 域名。

- 由于美利坚合众国政府实施经济、贸易和金融禁运的法律规定，古巴无法连接到围绕古巴群岛的光纤电缆，迫使古巴支付卫星服务，这种服务具有带宽的限制、获得必要技术的难题以及高昂的连接成本。
- 因特网被用来进行针对古巴的诽谤运动，以便颠覆和诋毁古巴。

14. 美国的这一态度，破坏了 2003 年和 2005 年世界各国在瑞士和突尼斯举行信息社会世界首脑会议时展现的精神、意愿和取得的成果。

15. 该首脑会议强烈敦促各国，在建设信息社会时采取措施，防止和避免采取不符合国际法和《联合国宪章》以及阻碍受影响国家人口充分实现经济社会发展和破坏其公民福利的单方面措施。

16. 联合国大会关于从国际安全的角度来看信息和电信领域发展的讨论很有意义，其时效性和重要性与日俱增。以上指出的美国对古巴采取的行动，说明了这一辩论很有必要，迫切需要找到制止这种表现的办法。

17. 古巴坚决支持联合国大会这一行动，将继续尽最大努力，促进全球和平发展信息技术和电信，并用之为全人类造福。古巴愿与包括美利坚合众国在内的其他国家进行协作，找到克服阻碍实现这些目标障碍的解决办法。

## 希腊

[原件：英文]

[2010 年 6 月 28 日]

1. 人们比过去任何时候都更广泛地讨论信息安全问题。随着全球化的到来，对于其固有的现代威胁的反措施当然也在考虑之列。还研究了维护信息自由流动的措施，以及在国内外采用这些措施的问题。
2. 遵循和研究了现有的国际和多国概念。需要提供评估风险的国际标准。应解决网络防卫的问题。应维护全球环境下，国家对信息安全的主权。
3. 据理解，所有会员国应继续向秘书长通报其对相关问题的意见和评估。在这方面，应注意下列几点：
  - (a) 所有信息安全问题均受到高度重视；
  - (b) 研究了采取何种方法维护信息的自由流通，提供必要程度的保密、完整性和可用性，并在国内外加以应用；
  - (c) 应草拟和商定国内国际分享网络链接的概念。必须进行网络链接风险评估，并提供有关国际指导准则。此外，由于各国一直严重关切采取措施保护网络安全的问题，必须制定统一的国际指导准则，以实现合作、效率和经济的目标。

最后但并非最不重要的是，不能忽视一个国家维护其主权以及维护其信息基础的要求，起草的每一个概念均应考虑到这一点；

(d) 为加强全球一级信息安全，国际社会可能采取的措施如下：

- (1) 详细拟定和商定有关国际概念；
- (2) 可拟定统一的通用基础设施的指导性计划，其中涵盖基本立法事项，以便向注册用户电子处理所有往来邮件和短信所需的信息安全，并提供多种通信方式；
- (3) 应统一和扩大多国联盟和小国群体所遵循的概念，并应用到全球。具体说明威胁及其负面影响的协定不应只是制定更复杂的措施，因为这些措施也可为对手所利用。
- (4) 与所有上述情况同样重要的是，应把国家的主权理解为全球化努力的基本参考要素。应制定和作为指南应用一种国际概念，即在反映出适宜程度的一体化背景下，界定国家信息交换的网关，以利于国家、多国和国际三级的努力。

## 墨西哥

[原件：西班牙文]

[2010年5月18日]

### 信息安全问题概况

1. 墨西哥银行和金融机构以及联邦政府处理安全和国家安全的单位，都是在计算机安全领域作出最大努力的机构。联邦公共安全秘书处内设有网络犯罪股和网络警察股。

2. 另一方面，虽然政府这三个部门分别进行了打击网络犯罪的努力，但联邦政府没有指导打击墨西哥网络犯罪的网络安全政策，必须加强这方面的立法，法官在处理和惩治网络犯罪方面需要更多的工具，需要加强针对因特网服务提供者的条例，要求他们保持在其平台上所有活动的记录，一旦事件发生，可提供信息。还有必要就打击网络犯罪和破坏国家安全的网路恐怖主义签署国内协定并与其他国家做出合作安排。

### 国家一级采取措施加强信息安全和促进在这一领域的国际合作

3. 墨西哥目前正努力查明信息安全的情况：

(a) 惩治某些网络犯罪可援引以下法律：《联邦刑法典》；《联邦区刑法典》；《刑事诉讼法》；《科洛马数据保护联邦法》；阿瓜斯卡连特斯、锡那罗亚、塔瓦斯科和塔毛利帕斯等州的《刑法》。

(b) 2009年4月30日，墨西哥《政府公报》公布一项法令，在墨西哥合众国《政治宪法》第73条加入第XXIX-0节，授权国会就保护人民所拥有的个人数据进行立法。

(c) 2009年6月，公布了一项法令，为《宪法》第16条增加了第2款，其中确认所有人都拥有保护其个人数据，有权以法律规定的方式，查阅、修改和删除这些数据并表达其反对意见。法律还提供了豁免以下原则的理由，即出于国家安全、法律和秩序、公众安全和健康或保护第三方权利的因素，指导数据处理工作的原则。

(d) 墨西哥国家自治大学计算机安全事故反应小组负责处理学术界安全问题，并在处理网络犯罪方面向墨西哥当局提供支持和技术咨询意见。

(e) 联邦警察部队设有网络警察单位，负责对公共安全犯罪行为进行后续调查工作。

(f) 政府正在编写一份关于网络脆弱性执行报告，以便通知政府高级部门全球网络事故的情况，从而组织和支持促进墨西哥网络安全的倡议。

(g) 计划在联邦政府内设立国家计算机安全事故应急小组(CSIRT)，<sup>1</sup>以协调打击国内外网络犯罪的努力。

(h) 网络脆弱性作为一个项目已列入国家风险议程。

(i) 在公共和私营部门的协调下，制定了提高普通公众对防止网络犯罪的认识的方案。

(j) 墨西哥参加了各种论坛，并与其他国家就网络犯罪问题签署了善意协定。

#### 国际社会加强全球信息安全可采取的措施

#### 4. 世界范围加强信息安全的措施如下：

(a) 通过适当的立法或根据需要更新现有立法，以保护网络空间的信息。

(b) 对法官进行网络安全问题的培训，使他们能够理解网络犯罪的性质，并作出适当判决。

---

<sup>1</sup> 计算机安全事故应急小组。

(c) 成立国家计算机安全事故反应小组，以协调各项努力，处理好重大安全事件，并作为其他国家的联络部门。

(d) 各国计算机安全事故反应小组之间不断进行联络，使其在区域或全球发生事故之际能协调各自的应对措施。

(e) 组织论坛，以分享经验并培训作为国际社会成员的各个安全小组。

(f) 为合作打击网络犯罪做出国际安排，以便利调查并形成团结战线。

## 巴拿马

[原件：西班牙文]

[2010年6月21日]

1. 巴拿马共和国设有支持出于包括恐怖行为内的犯罪目的，不适当利用因特网的机构，其中包括国家安全委员会、法治和秩序部内法医研究所。

2. 国家安全委员会从事的情报工作，是为了打击包括恐怖主义在内的有组织犯罪，以及有可能对财产和国家领土完整发动的攻击。

3. 根据2007年12月27日第69号法令，法医医学科学研究所设立了法律和秩序部，负责调查网络犯罪。

4. 我国《刑法典》规定利用因特网用于恐怖主义是犯罪行为，将予以镇压和惩治。第289条指出：“任何人使用因特网，实施恐怖主义行为提供训练，或招募他人予以实施，都将处以5至10年监禁。”

5. 其他法律法规也惩处出于犯罪目的利用因特网的行为，并规定将进行刑事、民事和行政处罚，其中包括2007年5月18日第14号法令第八章；2008年7月22日第51号法令第一章(计算机安全罪)，其中规范了电子文件及电子签名以及提供服务，并对电子贸易的发展作出了其他规定。1996年2月8日第38号法令颁布了指导巴拿马共和国电讯业的规则。

## 卡塔尔

[原件：英文]

[2010年5月25日]

1. 卡塔尔国认为应按照《联合国宪章》和国际关系基本原则使用信息和通讯技术。此外，保障信息的自由流通绝不应损害国家主权，同时应维护安全并尊重各国不同的文化、政治和道德。

2. 国家一级的努力基于通讯安全的利益，以随时加强之并跟上国内国际的进展。



### 3. 国内努力可简述如下：

- 制定安全战略和政策，颁布法律，限制出于不符合保护安全稳定目标的目的运用信通技术。
- 建立加强信息安全的机制，确保保护卡塔尔敏感信息的基础设施。
- 因特网安全和情报办公室努力监测政府网络和国家网络，以应对通过因特网对卡塔尔国形成的威胁。
- 对因特网事件加以管理并协调解决事件的努力，其目的在于在最短的停机时间内，保证把上报的有关因特网问题解决好。在卡塔尔国，这项工作由卡塔尔计算机应急小组负责。
- 让信息发挥更有效的作用，意识到改善卡塔尔各机构雇员的技术技能水平和资格。
- 支持卡塔尔人处理好与因特网有关的问题。
- 采取后续行动，理解现代科学技术领域与因特网安全有关的最新进展。
- 促进国际关系，以处理与因特网有关的问题。卡塔尔国参加了事故对应和安全小组论坛以及 Maridian 进程。

### 4. 国际社会为促进国家一级信息安全可采取的最重要措施如下：

- 联合国应继续领导这一讨论，并更多地澄清在电子战中使用信息、有线和无线通信技术的问题，现有国际法原则是否足以提供适当框架，以确定何为适当的在线行为，何为攻击性行径。
- 为建立有线和无线信息国际特设委员会，全面研究与此相关的问题。
- 卡塔尔国鼓励所有会员国建立工作队，在国家一级应对计算机紧急情况。
- 在通信领域，与专门的保安机构确定合同。
- 通过在地方和国际两级举行专题讨论会和会议，提高安全意识。
- 鼓励各国进行合作，以打击间谍活动和电子盗版活动。
- 使用加密和安全设备，以安全的方式转发信息和文件，以确保在交流时的保密性。
- 更新保护系统，定期举办讲习班，以盘点信息安全领域最新科技进展。

## 乌克兰

[原件：俄文]

[2010年5月12日]

1. 信息技术在社会各种活动中的作用日益扩大，导致人们担忧信息的安全。随着先进的信息技术进入各国社会的日常生活，犯罪份子以及试图犯罪的人对信息和电信系统、对国家机构信息资源以及对商业实体的网络攻击越来越多。
2. 计算机犯罪案中有一半涉及未经授权获取计算机信息。为获利而实施计算机犯罪的行为也越来越多，这种行为造成的物质损失也越来越大。跨国黑客集团犯罪数量也在增加。
3. 计算机犯罪很少报告，确定这类罪行全部范围的努力往往受挫。受到这种攻击的政府和商业实体总是试图掩盖事实，以免承担失去其权威的风险，他们不愿意透露所遭受的损失及其信息保障系统的薄弱。因此，这类犯罪案件往往得不到报案，这说明有必要制定协调一致的防范和预防措施，这些措施是保护信息系统的核心。
4. 计算机犯罪通常只是一系列犯罪行为的第一步，这与盗窃、勒索、诈骗等传统类型的罪行如出一辙。这些罪行日益变得更加复杂和隐蔽，其实施方式也日益精湛，给世界上几乎所有国家均造成巨大的经济和政治危害。此外，大多数专家认为各国的信息主权与国家安全事务之间存在直接联系。
5. 打击信息技术领域罪行的努力遇到许多具有法律性质的问题，因为计算机证据具有非物质以及经常是稍纵即逝的性质。在处理网络犯罪问题时所涉及的复杂问题使得国际合作更加重要。为此，所有国家最后还是要制定适当和相互兼容的法律、程序和规范类的工具。
6. 在实践中，对计算机犯罪的调查显示，迫切需要各国执法机构之间的合作。
7. 在国际实践中，通常采取联合措施调查计算机犯罪。乌克兰安全部门积极参与执法机构和特殊事务部门的联合行动，这也是打击通过因特网散播儿童色情制品以及国际恐怖主义诈骗罪的行动的一部分。
8. 此外，有必要加紧努力，进一步发展在提供信息安全方面的合作，维护共同利益和引进保护信息的措施，这主要是以双边和多边协议的形式。只有在各国政府机构有效合作的情况下，才能找到成功解决信息安全问题的办法，特别是因为所需的法律基础业已到位。
9. 鉴于有必要打击网络犯罪和网络恐怖主义的威胁，乌克兰安全局一直与外国执法机构保持接触。

10. 应指出，电脑犯罪分子往往选择政府办事处建立的网络作为其目标。此外，能否成功追查和惩治罪犯，取决于国际联系的质量，即是否已建立并优化了本国立法以符合当前的标准。

11. 考虑到计算机犯罪在全球持续增多，各国黑客集团之间存在联系以及网络威胁与国界无关，至关重要，应扩大在打击网络威胁的斗争中的合作。

12. 为执行信息社会世界首脑会议的各项决定(2003年12月10日至12日在日内瓦举行第一次会议；2005年11月16日至18日在突尼斯举行第二次会议)，乌克兰通过了一项关于2007-2015年乌克兰信息社会发展的基本原则法令。该法的目的是，在更加安全的环境内运用最新的信息和通讯技术。

13. 此外，已制定并通过了乌克兰电信发展计划。计划提供了后勤和技术保障，以确保乌克兰电信基础设施所有部门能安全运作，其中包括：

- 制定和逐步推行规范性和法律基础，以保护信息，通过技术手段和加密技术，保证符合欧洲和全球标准；
- 发展最新的信息保护方法，运用技术，全面解决保护电信网络资料的任务；
- 在法律允许的情况下，建立制度，合法拦截电信网络中的信息；
- 建立国家协调中心，协调公共信息和电信网络的安全，协助国家和非政府组织中心，回应和应对在这些网络上发生的事件。

14. 乌克兰对信息保护的规范性和法律依据还包括：国家安全的基本原则法令；信息法令；保护信息和电信系统的法令；总统和内阁成员关于从技术上保护乌克兰信息的发布令；信息、电信系统和网络的保护条例，与全球数据传输网络链接的程序。其中还包括了在司法部登记的大量规范性法规，宗旨是规范信息系统与全球数据传输网络的链接、特殊活动颁发执照的程序以及评估信息保护的程序。

15. 规范性和法律法规指出，只有使用受到保护的信息和通讯技术系统，才能对信息提供必要的保护，换句话说，应该使用那些纳入了综合信息保护系统的信息，这个单一系统包括一系列旨在应对威胁的法律和后勤措施、软件和硬件。综合系统及其信息保护组成部分必须经过认证以符合信息保护标准。

16. 为了规范综合信息保护系统的要求及其组成部分，乌克兰已制定并推出了约50个技术标准，规定了以下方面的准则：评估信息保护、信息和通信技术的分类、综合信息保护系统的每个组成部分达到信息保护要求的程序，这些均取决于所涉及各种不同的信息和通信技术、其最终目的、使用的领域和处理信息的类型。

17. 乌克兰也制定了本国评估信息技术安全的国家标准制度。该系统依据看一系列规范文书，即保护信息和电信系统免遭未经授权的获取该系统的信息；这些文

书已与欧洲联盟类似文书和国际标准统一，特别是国际标准化组织/国际电子技术委员会第 15408 号标准。

18. 此外，乌克兰还正在制定全国范围的组织和措施系统，以防止对国家机关、执法、海关和税务电信系统、信贷和金融机构等信息采取未经授权的行动，特别是企图通过因特网干扰其工作。

19. 按照《国家特别通讯和信息保护局法》第 16 条第 10 和 11 款的具体规定，为了加强国家机构之间的协调，以侦测对信息和电信系统进行的威胁，为了应对此种威胁实施的后果，并组织在这些问题上的国际合作，在该局内设立了适当的计算机应急小组，并已投入运作。

20. 计算机应急小组反映了全球对快速反应设施的行动趋势，计算机应急小组就是要应对计算机紧急情况。这类机构活动的国际协调由事故对应和安全小组国际论坛提供，这个论坛是应对安全事件的小组的论坛。

21. 2009 年 7 月 13 日，乌克兰计算机应急小组成为该论坛的正式成员 ([www.cert.gov.ua](http://www.cert.gov.ua))。

22. 2009 年，乌克兰应急小组处理了来自 30 个国家和地区计算机应急小组的 461 份报告(澳大利亚、奥地利、比利时、加拿大、中国、丹麦、芬兰、法国、爱沙尼亚、德国、匈牙利、印度、以色列、意大利、日本、韩国、立陶宛、马来西亚、荷兰、挪威、巴基斯坦、波兰、葡萄牙、罗马尼亚、俄罗斯联邦、沙特阿拉伯、西班牙、中国台湾、土耳其、美利坚合众国)，其中涉及在乌克兰因特网从事的未经授权行为(分发有害软件、发动“拒绝服务”攻击及其他企图犯下的未经授权的行为)。

23. 还应指出的是，乌克兰建立了法律和监管框架，并确保国家特别通讯和信息保护服务局与执法机构之间的合作，以采取措施，保障信息和电信系统中国家信息资源的安全，提高该系统的能力，以应对那些未经授权的针对信息资源的行为。

24. 因此，在乌克兰建立信息和电信系统的所有阶段及其综合信息保护系统中的信息现均可得到保护，无论处理的信息的种类如何重要性如何，以及无论信息和电信系统的种类和复杂性如何。此外，制定整个信息和电信系统的信息资源的要求、设计、开发、安全评估以及保护的所有基本办法，均符合联合国会员国以及欧洲联盟成员国的国家安全部门采用的方法。

25. 为了培训信息安全和计算机工程领域的专家，成立了信息保护研究所，这是国家信息和通讯技术大学的一个学术和科学部门。

## 大不列颠及北爱尔兰联合王国

[原件：英文]

[2010年6月2日]

1. 联合王国高兴地对有关从国际安全的角度来看信息和电信领域的发展的联合国第64/25号决议，做出回应。

2. 我们认为这个问题极为重要，关系到每个国家在国际安全大环境中的商贸和对本国公民的保护。联合王国尽了相当大的努力，使网络空间对于所有国家而言，更为安全，我们欢迎在这一领域的国际活动，我们相信所有国家应进行合作，以促进网络空间有个安全、复原力强的环境。

### 对信息安全问题的一般看法

3. 我们相信，一个安全的网络空间对于当今世界非常重要。公民、商业、重要的国家基础设施和政府越来越多地依赖于因特网。影响某国因特网服务的任何事件都有可能对该国产生后果，也许还是严重的后果。遗憾的是，任何国家内外都可能出现若干威胁行动者，他们可能会出于某些原因，试图扰乱或操纵因特网服务。

### 在国家一级为加强信息安全和促进这一领域的国际合作而采取的努力

4. 联合王国将继续在国内外努力，以促进网络空间的安全。在国内，我们于2009年6月出版了《国家网络安全战略》。该文件加强了全国关于信息安全的努力。该《战略》要求成立2个新的组织，网络安全办公室和网络安全行动中心。这两个组织已经成立，并继续扩大。联合王国有3个计算机应急小组，向联合王国关键基础设施、军事和其他政府网络提供专家服务。在国际范围，我们也积极参与这项工作。我们在联合国的参与包括参加政府专家小组。我们是关于创建全球网络安全文化以及评估各国保护重要信息基础设施的努力的联合国决议的共同提案国。我们是国际电信联盟(国际电联)有关机构的成员。我们参加了欧洲安全与合作组织的各项活动。在我们的全力支持和参与下，欧盟已开始对保护欧盟各国重要的基础设施的若干倡议开展工作。我们参加了欧盟与东盟的接触，参加了东盟关于网络安全的区域论坛。同样，我们还参与了北约内部一些有关保护该组织网络的活动。联合王国一直是MERIDIAN进程([www.meridian2007.org](http://www.meridian2007.org))、事故对应和安全小组论坛([www.first.org](http://www.first.org))和欧盟各国计算机应急小组组织的牵头国家([www.egc-group.org](http://www.egc-group.org))之一。

5. 联合王国国家网络安全战略可从内阁网页[www.cabinetoffice.gov.uk](http://www.cabinetoffice.gov.uk)下载。

### 国际社会为加强全球一级的信息安全可能采取的措施

6. 我们鼓励所有国家设立计算机应急小组。我们鼓励所有国家制定有关网络犯罪的有效的国内立法。我们相信，电子犯罪不是网络空间的唯一罪恶活动，但是

最普遍的活动。我们认为减少犯罪活动将有利于所有人。我们认为，欧洲委员会《网络犯罪公约》代表了打击国际电子犯罪的合适工具。此外，我们相信，国际电联开发、联合国推广的工具包为各国提供了自我评估准备解决对重要的国内基础设施潜在攻击的良好基础。我们欢迎在多种场合，为促进信息安全最佳实践做出的努力。

#### 有关国际概念

7. 主要的国际概念是国际法的概念。对现有国际法律是否适用于网络空间，有过相当多的辩论、尤其是在网络会议上。联合王国已研究过这个问题，我们的观点是，有关使用武力和武装冲突法的现有国际法原则，为查明和分析利用网络空间从事敌对行动，提供了合适的框架。

---